



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
[www.uspto.gov](http://www.uspto.gov)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/833,634	04/13/2001	M. Paul Zavidniak	026590-006	3065

7590                    12/17/2004

Richard J. McGrath  
BURNS, DOANE, SWECKER & MATHIS, L.L.P.  
P.O. Box 1404  
Alexandria, VA 22313-1404

EXAMINER

MILLER, BRANDON J

ART UNIT

PAPER NUMBER

2683

DATE MAILED: 12/17/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	09/833,634	ZAVIDNIAK, M. PAUL	
	Examiner Brandon J Miller	Art Unit 2683	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

#### Status

- 1) Responsive to communication(s) filed on 06 August 2004.
- 2a) This action is FINAL.                    2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

#### Disposition of Claims

- 4) Claim(s) 1-15 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) Claim(s) \_\_\_\_\_ is/are allowed.
- 6) Claim(s) 1-15 is/are rejected.
- 7) Claim(s) \_\_\_\_\_ is/are objected to.
- 8) Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

#### Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on \_\_\_\_\_ is/are: a) accepted or b) objected to by the Examiner.  
 Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
 Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

#### Priority under 35 U.S.C. §§ 119 and 120

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
 a) All b) Some \* c) None of:  
 1. Certified copies of the priority documents have been received.  
 2. Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.
- 13) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application) since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.  
 a) The translation of the foreign language provisional application has been received.
- 14) Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121 since a specific reference was included in the first sentence of the specification or in an Application Data Sheet. 37 CFR 1.78.

#### Attachment(s)

- 1) Notice of References Cited (PTO-892)                    4) Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_.  
 2) Notice of Draftsperson's Patent Drawing Review (PTO-948)                    5) Notice of Informal Patent Application (PTO-152)  
 3) Information Disclosure Statement(s) (PTO-1449) Paper No(s) \_\_\_\_\_.                    6) Other:

## DETAILED ACTION

### *Response*

#### *Claim Rejections - 35 USC § 103*

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

- (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-3, 10, and 13 are rejected under 35 U.S.C. 103(a) as being unpatentable over Huff view of Vaidya.

Regarding claim 1 Huff teaches a method of detecting intrusions in a wireless network (see col. 13, lines 44-49 and col. 14, lines 16-20). Huff teaches researching and defining normal network behavior with the intent of ascertaining user and temporal patterns (see col. 10, lines 27-28 & 32-37). Huff teaches researching potential sources of information that will lead to the detection and classification of potentially intrusive events (see col. 10, lines 54-56). Huff teaches establishing a knowledge base of anomalous network activity that will form the foundation for classifying potentially intrusive events (see col. 7, lines 52-57). Huff teaches analyzing and evaluating a knowledge base to dispatch countermeasure agents; and utilizing the countermeasure agents to provide an adaptive response to intrusions in the network (see col. 10, lines 54-67 and col. 11, line 1). Huff does not specifically teach creating an attack model. Vaidya teaches creating an attack model (see col. 7, lines 36-37 & 42-45). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the

countermeasure in Huff to include creating an attack model because this would allow for an alternative device that detects and prevents unauthorized network access.

Regarding claim 2 Huff teaches collecting real-world information concerning potentially intrusive events and updating the knowledge base (see col. 7, lines 52-55).

Regarding claim 3 Huff teaches developing a recovery model to recover from an intrusion of the network (see col. 10, lines 61-67 and col. 11, line 1).

Regarding claim 10 Huff teaches data related to suspicious events including passive eavesdropping, deception and denial of service (see col. 7, lines 52-55 and col. 12, lines 25-34).

Regarding claim 13 Huff teaches a method of detecting intrusions in a wireless network (see col. 13, lines 44-49 and col. 14, lines 16-20). Huff teaches researching and defining normal network behavior with the intent of ascertaining user and temporal patterns (see col. 10, lines 27-28 & 32-37). Huff teaches researching potential sources of information that will lead to the detection and classification of potentially intrusive events (see col. 10, lines 54-56). Huff teaches augmenting the researching step by collecting real-world information concerning intrusive events and updating the knowledge base (see col. 7, lines 52-54). Huff teaches establishing a knowledge base of anomalous network activity that will form the foundation for classifying potentially intrusive events (see col. 7, lines 52-57). Huff teaches analyzing and evaluating a knowledge base to dispatch countermeasure agents; and utilizing the countermeasure agents to provide an adaptive response to intrusions in the network (see col. 10, lines 54-67 and col. 11, line 1). Huff teaches developing a recovery model to recover from an intrusion of the network (see col. 10, lines 61-67 and col. 11, line 1). Huff does not specifically teach creating an attack model. Vaidya teaches creating an attack model (see col. 7, lines 36-37

& 42-45). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the countermeasure in Huff to include creating an attack model because this would allow for an alternative device that detects and prevents unauthorized network access.

Claims 4-9, 12, and 14-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Huff in view of Vaidya and Hopkins.

Regarding claim 4 Huff and Vaidya teach a device as recited in claim 1 except for a wireless network that is the Tactical Internet. Vaidya does teach a network that is the Internet (see col. 5, lines 44-46). Hopkins teaches tactical data links exchanging messages in a radio network (see pg. 5, 9<sup>th</sup> paragraph and pg. 6, 1<sup>st</sup> paragraph). It would have been obvious to one of ordinary skill in the art at the time the invention was made to make the device adapt to include a wireless network that is the Tactical Internet because this would allow for improved detection and prevention of Internet access from fraudulent users.

Regarding claim 5 Huff, Vaidya, and Hopkins teaches a device as recited in claim 1 except for a wireless network that is a Situation Assessment Data Link (SADL). Hopkins does teach a wireless network used to analyze data link messages (see pg. 4, 1<sup>st</sup>-3<sup>rd</sup> paragraphs). It would have been obvious to one of ordinary skill in the art at the time the invention was made to make the device adapt to include a wireless network that is a Situation Assessment Data Link (SADL) because this would allow for efficient recovery from network intrusion.

Regarding claim 6 Hopkins teaches a wireless network that is a tactical data link network (see pg. 5, 9<sup>th</sup> paragraph and pg. 6, 1<sup>st</sup> paragraph).

Regarding claim 7 Hopkins teaches a tactical data link that is a Link-16 type tactical data link and its logical extensions (see pg. 6, 1<sup>st</sup> paragraph).

Regarding claim 8 Hopkins teaches a device as recited in claim 7 and is rejected given the same reasoning as above.

Regarding claim 9 Hopkins teaches a device as recited in claim 7 and is rejected given the same reasoning as above.

Regarding claim 11 Vaidya teaches an attack model that is utilized to generate signatures of suspicious events (see col. 5, lines 33-36).

Regarding claim 12 Vaidya teaches an attack model that is utilized to generate recommendations regarding the set up of a network (see col. 6, lines 10-18).

Regarding claim 14 Huff teaches a method of detecting intrusions on a computer network (see col. 13, lines 44-49 and col. 14, lines 16-20). Huff teaches researching and defining normal network behavior with the intent of ascertaining user and temporal patterns (see col. 10, lines 27-28 & 32-37). Huff teaches researching potential sources of information that will lead to the detection and classification of potentially intrusive events (see col. 10, lines 54-56). Huff teaches establishing a knowledge base of anomalous network activity that will form the foundation for classifying potentially intrusive events, wherein the knowledge base includes data relating to suspicious events including passive eavesdropping, deception and denial of service (see col. 7, lines 52-57 and col. 12, lines 25-34). Huff teaches augmenting the researching step by collecting real-world information concerning intrusive events and updating the knowledge base (see col. 7, lines 52-54). Huff teaches analyzing and evaluating a knowledge base to create IW countermeasure agents; and utilizing the IW countermeasure agents to provide an adaptive response to intrusions in the network (see col. 10, lines 54-67, col. 11, line 1, and col. 14, lines 40-42). Huff teaches developing a recovery model to recover from an intrusion on the network

(see col. 10, lines 61-67 and col. 11, line 1). Huff does not specifically teach detecting intrusions in the Tactical Internet or creating an attack model. Vaidya teaches creating an attack model (see col. 7, lines 36-37 & 42-45). Vaidya teaches a network that is the Internet (see col. 5, lines 44-46). Hopkins teaches tactical data links exchanging messages in a radio network (see pg. 5, 9<sup>th</sup> paragraph and pg. 6, 1<sup>st</sup> paragraph). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention to include detecting intrusions in the Tactical Internet and creating an attack model because this would allow for an alternative device that detects and prevents unauthorized Internet access.

Regarding claim 15 Huff teaches a method of detecting intrusions on a network (see col. 13, lines 44-49 and col. 14, lines 16-20). Huff teaches researching and defining normal network behavior with the intent of ascertaining user and temporal patterns (see col. 10, lines 27-28 & 32-37). Huff teaches researching potential sources of information that will lead to the detection and classification of potentially intrusive events (see col. 10, lines 54-56). Huff teaches establishing a knowledge base of anomalous network activity that will form the foundation for classifying potentially intrusive events, wherein the knowledge base includes data relating to suspicious events including passive eavesdropping, deception and denial of service (see col. 7, lines 52-57 and col. 12, lines 25-34). Huff teaches augmenting the researching step by collecting real-world information concerning intrusive events and updating the knowledge base (see col. 7, lines 52-54). Huff teaches analyzing and evaluating a knowledge base to create IW countermeasure agents; and utilizing the IW countermeasure agents to provide an adaptive response to intrusions in the network (see col. 10, lines 54-67, col. 11, line 1, and col. 14, lines 40-42). Huff teaches developing a recovery model to recover from an intrusion on the network (see col. 10, lines 61-

67 and col. 11, line 1). Huff does not specifically teach detecting intrusions in a RF based tactical data link or creating an attack model. Vaidya teaches creating an attack model (see col. 7, lines 36-37 & 42-45). Vaidya teaches a network that is the Internet (see col. 5, lines 44-46). Hopkins teaches a wireless network that is a tactical data link network (see pg. 5, 9<sup>th</sup> paragraph and pg. 6, 1<sup>st</sup> paragraph). It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the invention to include detecting intrusions in a RF based tactical data link or creating an attack model because this would allow for an alternative device that detects and prevents unauthorized access in of a RF data link.

***Response to Arguments***

Applicant's arguments with respect to claims 1-15 have been considered but are moot in view of the new ground(s) of rejection.

***Conclusion***

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Sawyer U.S Patent No. 6,073,006 discloses a method and apparatus for detecting and preventing fraud in a satellite communication system.

Ferrel U.S Patent No. 5,005,210 discloses a method and apparatus for characterizing a radio transmitter.

Martin U.S Patent No. 6,772,349 B1 discloses detection of an attack such as a pre-attack on a computer network.

Porras U.S Patent No. 6,321,338 discloses network surveillance.

Froutan U.S Patent No. 6,654,882 discloses a network security system protecting against disclosure of information to unauthorized agents.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brandon J Miller whose telephone number is 703-305-4222. The examiner can normally be reached on Mon.-Fri. 8:00 am to 5:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William Trost can be reached on 703-308-5318. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

November 5, 2004



WILLIAM TROST  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2600